

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 12135-006001	Application No. 09/788,670
		Applicant Soeren LAURSEN et al.	
		Filing Date February 21, 2001	Group Art Unit 2121 2124

**Information Disclosure Statement
by Applicant**
(Use several sheets if necessary)

(37 CFR §1.98(b))

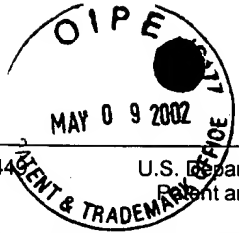
U.S. Patent Documents							
Examiner Initial	Desig. ID	Patent Number	Issue Date	Patentee	Class	Subclass	Filing Date If Appropriate
CD	AA	4,928,223	5/22/90	Dao et al.			
CD	AB	5,499,299	3/12/96	Takenaka et al.			
CD	AC	5,748,979	5/5/98	Trimberger			
CD	AD	6,009,450	12/28/99	Dworkin et al.			
CD	AE	6,035,317	3/7/00	Guy			
CD	AF	6,067,615	5/23/00	Upton			
CD	AG	6,138,229	10/24/00	Kucukcakar et al.			
CD	AH	6,141,421	10/31/00	Takaragi et al.			
CD	AI	6,154,834	11/28/00	Neal et al.			
	AJ						
	AK						

RECEIVED
MAY 10 2002
Technology Center 2100

Foreign Patent Documents or Published Foreign Patent Applications								
Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation	
							Yes	No
	AL							
	AM							
	AN							
	AO							
	AP							

Other Documents (include Author, Title, Date, and Place of Publication)		
Examiner Initial	Desig. ID	Document
CD	AQ	Jae Wook Chung et al., <i>Fast Implementation of Elliptic Curve Defined over $GF(p^m)$ on CalmRISC with MAC2424 Coprocessor</i> , C.K. Koc and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 57-70, 2000.
CD	AR	Darrel Hankerson et al., <i>Software Implementation of Elliptic Curve Cryptography over Binary Fields</i> , C.K. Koc and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 1-24, 2000.
CD	AS	Marc Joye et al., <i>Efficient Generation of Prime Numbers</i> , C.K. Koc and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 340-354, 2000.
CD	AT	Souichi Okada et al., <i>Implementation of Elliptic Curve Cryptographic Coprocessor over $GF(2^m)$ on an FPGA</i> , C.K. Koc and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 25-40, 2000.

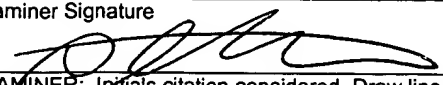
Examiner Signature 	Date Considered 8/5/03
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	



Substitute Form PTO-1449 (Modified) Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 12135-006001	Application No. 09/788,670
		Applicant Soeren LAURSEN et al.	
	Filing Date February 21, 2001	Group Art Unit 2121 2124	

Other Documents (include Author, Title, Date, and Place of Publication)		
Examiner Initial	Desig. ID	Document
CD	AU	Geraldo Orlando et al., <i>A High-Performance Reconfigurable Elliptic Curve Processor for GF(2^m)*</i> , C.K. Koc and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 41-56, 2000.
CD	AV	Erkay Savas et al., <i>A Scalable and Unified Multiplier Architecture for Finite Fields GF(p) and GF(2^m)*</i> , C.K. Koc and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 277-292, 2000.
CD	AW	Zhijie Shie et al., <i>Bit Permutation Instructions for Accelerating Software Cryptography</i> , Proceedings of the IEEE International Conference on Application-specific Systems, Architectures and Processors, July 10-12, 2000, Boston, Massachusetts, USA, pp. 138-148.

RECEIVED
MAY 10 2002
Technology Center 2100

Examiner Signature 	Date Considered 8/5/03
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	